

11.3.7 Details on the Messaging Services Proposed Solution

Solution Overview

The Commonwealth Partners propose a centralized, Microsoft technology based solution to include Microsoft Active Directory and Microsoft Exchange Server 2003 as the core directory and messaging services. Microsoft Active Directory and Exchange 2003 environments have proven records of accomplishment for high-availability solutions in large enterprise environments containing millions of directory objects and hundreds of thousands of mailboxes.

Today, the United States Army and the Department of Justice, each with sub agencies that have different business and security requirements similar to those of the Commonwealth of Virginia, use this Microsoft technology based solution.

A major benefit of choosing the Microsoft technology based solution is to reduce migration risks, migration costs, administrative training costs, and end user training costs. This is because more than 50% of the Commonwealth agencies are already using Microsoft infrastructures.

The Messaging solution meets all of the Commonwealth requirements focusing on improved end-user productivity through highly available services with built-in redundancies and improved security.

Other platforms were researched for the Commonwealth solution, however they proved to be more costly and would not attain the technical requirements stated in the SOW.

Solution Description

The Commonwealth Partner's solution incorporates all the requirements of the scope of work to accomplish the Commonwealth's goals. The following technologies are implemented to provide the services required in Figure 11.3.7 - 1 below.

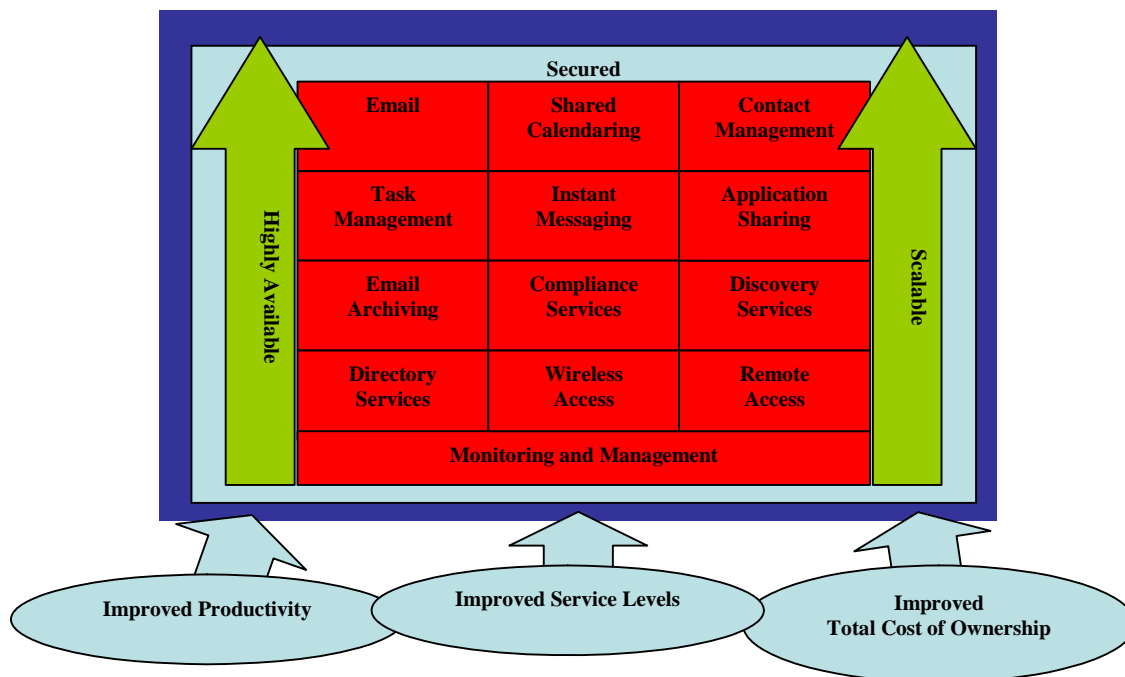


Figure 11.3.7 - 1 Implemented Technologies provide required services.

The Commonwealth Partners Solution offers the following:

1. Microsoft Cluster Servers
 - a. High Availability
2. Cisco Load Balancing
 - a. High Availability
3. IBM X-Series four processor servers
 - a. Scale Up capabilities
4. Microsoft Active Directory
 - a. Directory Services
 - b. Security
 - c. Scale Out capabilities
5. Microsoft Exchange Server 2003 with Outlook Web Access
 - a. Email
 - b. Shared Calendaring
 - c. Contact Management
 - d. Task Management
 - e. Remote Access
 - f. Scale Out capabilities
6. Microsoft Live Communication Server 2005*
 - a. Instant Messaging
 - b. Application Sharing
 - c. Ad Hoc Online Meetings
 - d. Whiteboard Sharing
 - e. Scale Out capabilities
7. Ilumin Assentor*
 - a. Compliance Services
 - b. Email Archiving
 - c. Discovery Services
 - d. Scale Out capabilities
8. RIM Blackberry Enterprise Server*
 - a. Wireless Access
 - b. Scale Out capabilities
9. Quest Monitoring and Management Tools
 - a. Monitoring and Management
 - b. Scale Out capabilities

10. Verisign Certificates

- a. SSL Encryption for Remote Access
- b. S/MIME Encryption for email clients

**Indicates solutions that are not part of the base offering, but can be added at a per user choice by the agencies.*

Benefits/ Future State

Today, communication and access to information is probably the most critical requirement of any job. Workers must be able to communicate with management, peers, and customers quickly and constantly to meet expectations and requirements. The technology implemented for the Commonwealth gives agencies and workers access to the information they need, whenever and wherever they need it.

Other benefits include:

- 1. More secure communications
- 2. Greater Return on Investment
- 3. Increased flexibility and usability of end user tools
- 4. Increased methods of access to the core communication tools
- 5. Increased capability to retain and manage agency specific knowledge
- 6. Increased system up time to allow for less user work interruption
- 7. Lower overall total cost of ownership

The Commonwealth Partners have created a messaging architecture that meets the Commonwealth's messaging requirements. This robust architecture is based on industry-proven technologies that will provide flexibility, scalability, and reliability at every level. These include Microsoft Active Directory and Microsoft Exchange Server 2003, which serve as the core components of the Commonwealth's future messaging system. The architecture also includes high-performance IBM xSeries quad processor servers, which will be load balanced and clustered for consistent system performance, redundancy, and high availability.

The following graphic Figure 11.3.7 - 2 depicts the overall solution architecture.

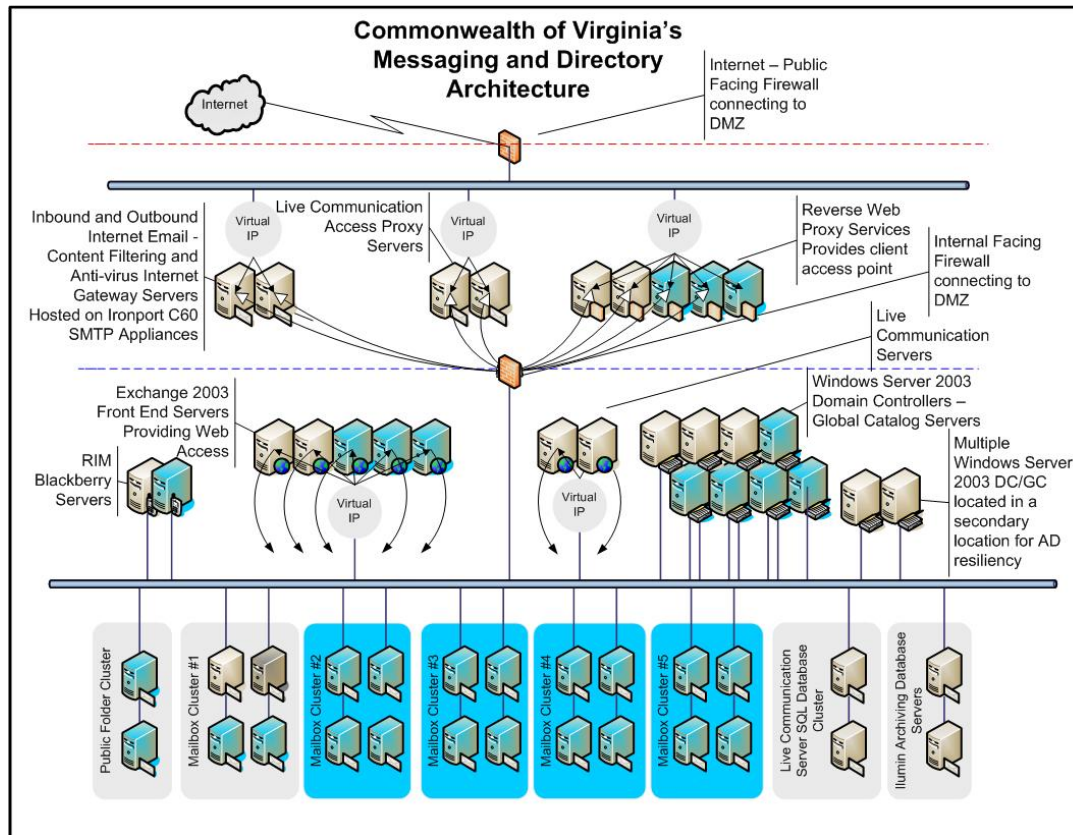


Figure 11.3.7 – 2 Overall Solution Architecture

Figure 11.3.7 – 3 contains a summary of the Technology used to meet the Messaging Solution and Service Offering objectives and requirements.

Software	Functional Description
Pre-Migration Activities	
Microsoft Active Directory on Windows 2003	Provides security context within the Active Directory “Forest”. Holds user accounts, user attributes, Exchange 2003 information, workstation accounts, server accounts, Group Policy Objects (GPO), and other domain management functions.
Microsoft Exchange 2003	Provides databases and storage structure for user mailboxes. Creates Global Address Lists and agency level address lists. Sets mailbox size limits, SMTP addressing, public folder size limits, and other messaging policy functions.
Symantec for Exchange 2003	Provides antivirus protection services for the internal messaging systems.
*Microsoft Live Communication Server 2005	Provides real-time collaboration by using instant messaging, presence detection, application sharing, whiteboard sharing, and other collaboration capabilities.

Software	Functional Description
*Illumin Assessor Enterprise with compliance, discovery, and archiving service options	Provides compliance scanning for inappropriate use of email. Provides discovery search capability for legal searches. Provides archiving for email messaging and allows users to access those archives.
Ironport C60 SMTP gateway appliances	Blocks SPAM from entering the internal messaging systems. Quarantines or cleans virus infected emails. Reports on Internet traffic patterns.
Spotlight on Active Directory	Provides Active Directory database replication monitoring and alerts. Monitors physical hardware to discover bottlenecks before they become performance problems.
Spotlight on Exchange	Provides Exchange server monitoring and alerts. Monitors delivery time and overall performance of Exchange servers.
MessageStats	Reports on total cost of ownership concerns within Exchange. Provides chargeback data for mailbox size, system usage per user, or other counters.
**Migration Manager for Active Directory	Automates coexistence and migration between two Active Directory forests.
**Migration Manager for Exchange	Automates coexistence and migration between two Exchange 2000 and 2003 organizations.
**Exchange Migration Wizard	Automates coexistence and migration between Exchange 5.5 organizations and Exchange 2000 or 2003 organizations.
**Novell Directory Service Migrator	Automates coexistence and migration from Novell Directory Services to Active Directory.
**Groupwise Migrator	Automates coexistence and migration from GroupWise to Exchange 2000 or 2003.
**Notes Migrator	Automates coexistence and migration from Domino/Lotus Notes to Exchange 2000 or 2003.
Microsoft SQL Server 2000	Supports databases for the tools and software that require SQL database support.

Figure 11.3.7 - 3 Software used for the Commonwealth's architecture to include migration and monitoring software

**Indicates solutions that are not part of the base offering, but can be added at a per user choice by the agencies.*

***Indicates software tools that will be used only within specific migration contexts, depending on the agency legacy system type. Also dependent upon the level of migration that the agency chooses.*

Migration strategy

The Commonwealth Partners have a detailed strategy on how to manage the legacy operations, new operations, and migration between the two operational systems while maintaining the integrity and service levels of both environments. This strategy is formulated to ensure the use of experienced staff when and where needed to mitigate risk.

The migration team has experience in migrating a wide variety of messaging and directory systems to Microsoft Active Directory and Exchange architectures with predictable and dependable results. This migration experience includes large geographically dispersed environments such as the United States Army.

The migration plan high-level overview migrates all current agency systems into the current VITA Exchange 2003 and Active Directory environment. The current VITA environment is assumed to have the necessary architecture to handle the addition of all agencies to this centralized solution, though new hardware will be built out by the Commonwealth Partners to support the entire Commonwealth. The Messaging operations team adds the necessary services to the architecture so the environment scales appropriately without slowing migration efforts.

The example migration timeline below gives an approximation of how the agency migrations may be performed. Several agency migrations begin concurrently, but then close out at different times. As each migration is closed out, other planning phases will already have begun. Each agency has their own unique set of circumstances and requirements that either extends or decreases the timeline for that individual agency.

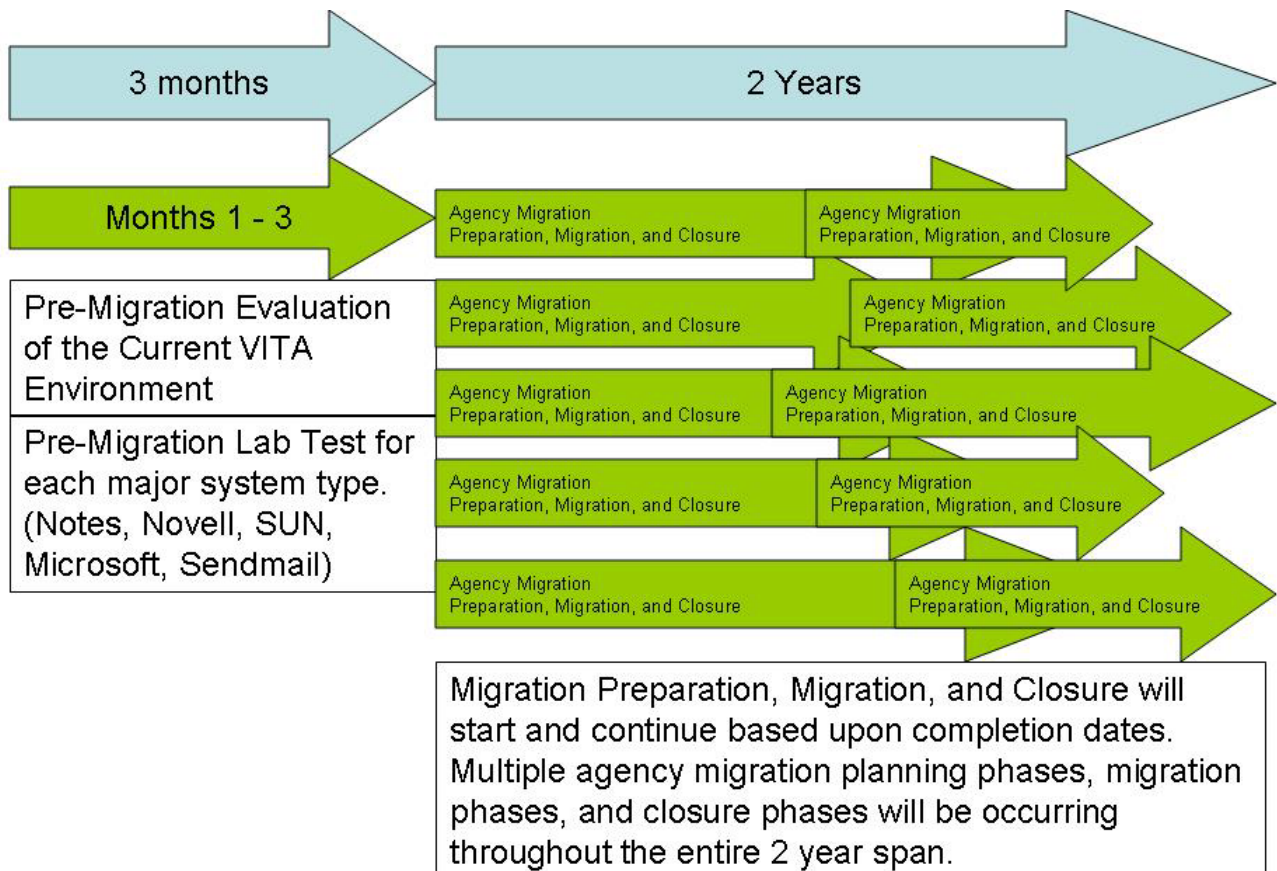


Figure 11.3.7 - 4 Sample agency migration timeline

The Commonwealth Partners developed a detailed and flexible migration strategy offering a choice of migration options for each agency. The choice offerings follow the same project plans and methodologies, however specific tasks and software costs are included or excluded as required by the agencies. It is important to note that each agency will have specific requirements based on the technology they have implemented. The detailed individual steps for each migration will be documented during the migration-planning phase; it is at that time that the agency should make these option choices. The offering choices are summarized below.

Option 1 – Bronze Level Migration – (Baseline for 50% of Population)

The Bronze Level Migration option is tailored specifically for those agencies currently using Exchange email servers for their mailboxes today. Based on due diligence information, this encompasses roughly 50% of the total agency population. The Bronze Level Migration Option includes these services:

- All necessary user objects from the legacy agency directory will be copied to the new Active Directory environment for each user during their scheduled migration.
- New, empty mailboxes for each user will be created in the new Exchange 2003 environment.
- The end user will be given instructions to download their email from their legacy email servers to their local machines saving it as an archived PST file for future viewing in the new environment.
- The end user will be given instructions on how to change their Outlook email client configuration to connect to their new empty mailbox.

This Bronze level Migration assumes most of these users already have the Outlook client installed on their machine. However, if this is not the case, the Commonwealth Partners will ensure this is done prior to the users' scheduled migration. If legacy Exchange users do not want to copy their email to their local machines for any reason, they may prefer the Silver Level Migration Option instead.

Option 2 – Silver Level Migration – (Baseline Option for Remaining 50% of Population)

The Silver Level migration is tailored specifically for those agencies using non-Microsoft email solutions today. Based on due diligence information, this encompasses the remaining 50% of the total agency population. The Silver Level Migration Option includes everything listed in the Bronze Level Migration option described above plus these additional services:

- Users' server-side mailbox data will be migrated from their legacy email servers to their new mailbox on the new Exchange 2003 server.
- Users will be given instructions on how to convert their local archives from legacy clients to new Outlook PST archives.

This Silver Level Migration Option includes user's email up to 40 MB mailbox sizes. Users with mailboxes exceeding the 40 MB mailbox size will be looked at on a case-by-case basis to determine proper handling to meet the user requirement while also minimizing the impact of the requirement on the overall migration schedule.

Option 3 – Gold Level Migration (Full Service)

Realizing the hectic schedules of busy executives, the Commonwealth Partners developed a Gold Level Migration Option tailored for those users that require the "white glove", full service offering. These users may prefer to have their email clients reconfigured for them. Or, perhaps they have a unique requirement with their local archives whereby they need extra assistance and/or full desk side support in converting

the local archives for them. Although this “white glove” option is not part of the core service offering, it is available for those that need it.

Operations & Migration strategy

The Commonwealth Partners have a detailed plan on how the operations and migrations of the Commonwealth agencies will be handled as it relates to messaging and directory services. The processes are described within the following table.

Process	Description
Assume business as usual operations.	All current operational staff will continue to maintain normal operations within their individual agencies until migration is scheduled.
Initial migration team to evaluate all current infrastructures to ensure environment is ready for migration.	This includes the current VITA Active Directory and Exchange 2003 environments. The Commonwealth Partners would like to use this environment as the target for all migrations; therefore an understanding of the environment will be required, to include naming conventions, DNS structure, etc. Changes to this existing VITA architecture are not expected or planned for within the Commonwealth Partner’s plan.
Create Lab environment and test processes and procedures.	The migration team will build out a lab that allows each type of migration to be tested. This serves as a proof of concept lab throughout the migration timeline and ensures the quality of the migrations.
Operations team for the target operational environment.	This team keeps the target directory and messaging systems healthy and scales the environment throughout the migration. This team integrates all monitoring, reporting, and other administrative functions with each newly migrated agency.
Install new SAN and X-Series hardware to the Richmond Plaza data center.	The Messaging operations team in cooperation with the Midrange tower builds initial environment used by the agency. The operations team in the existing Commonwealth RPB data center builds the migration environment including OWA servers, Live Communication Servers, Quest Management Tools, Microsoft SQL Server Clusters, Exchange Back End Mailbox Clusters, and others.
Schedule migrations for four or more agencies at a time for the 2-year migration project.	Non-Microsoft infrastructure systems will be targeted as soon as possible due to the fact that they have the Silver option baseline, which is a longer migration process. However, scheduling of agency migrations will be based upon an agreed upon strategy which will be detailed upon award and commencement. There will be several dependencies that cross tower requirements and most importantly agency business requirements before the final schedule can be determined.
Agency migration planning and execution	
Attain workstation report from Desktop tower to ensure workstations conform to minimum requirements for any migration option.	The Desktop tower determines the workstation conditions of each agency and ensures workstations that do not meet the minimum standards are brought up to the minimum standards before the migration of the agency starts. The minimum requirements for desktops are shown in Table 1.3 below. Workstations that do not fulfill the minimum requirements can be patched, upgraded, refreshed, or re-imaged as necessary by the desktop tower personnel through the use of their normal support procedures.

Process	Description
Examine and report conditions of all messaging and directory servers within the agency environment.	Evaluation for patches, upgrades and re-structuring may be required in some environments to ensure successful migrations.
Setup communications plan with all stakeholders.	Stakeholders within the Commonwealth's messaging migrations consist of agency personnel, within VITA, and within the Commonwealth Partners. Groups such as, the Help Desk tower, Midrange tower, Security tower, Cross functional tower, Desktop tower, agency management, Messaging tower, and several more will be involved with the communications plan.
Schedule user migrations with primary point of contact in agency.	Meet with POC to develop a schedule of all the mailboxes for the agency.
Copy all user objects and mail attributes from current system to the new system.	This is a function of the Quest migration tools being used for the migrations providing the new system with a populated Global Address List of all users within the agency being migrated. Their email addresses point to their legacy system mailboxes.
Conduct pilot migration of selected agencies that represent the primary migration scenarios.	Migrate the identified pilot users. This migration copies the mail data from the legacy system to the new system and re-points the users mail addresses within both legacy and new directory systems to the new location. The users will be given instructions to change their Outlook clients to connect to the user's new Exchange server. Any local archives not in Outlook format can be converted by the end user using provided instructions. The Help Desk tower will have staff capable of assisting users in these efforts, and clear instructions and schedules will be provided to them as well.
Conduct production migrations.	Migrations begin. The migration team migrates up to 150 users per day across all agencies ensuring the two-year project timeline is achieved. The 150 users per day is an overall average forecast.
Add services to users selected by the agency.	When a group of users migrates to the new solution, the operations team knows what services the agency selected for those users. New services like Live Communication Server (LCS) or Illumin Assentor Enterprise will be added to these user accounts when they are added to the new system. (Note: LCS requires Windows XP desktop with Office 2003 and Microsoft Communicator.)
Conduct migration project closure.	Confirm with the agency POC that all user mailboxes have been migrated.
Migration team members move to next agency migration.	The migration team members that conducted the migration move to the next agency for planning.
Retire legacy systems no longer required.	Shutdown and repurpose, or dispose of the legacy systems messaging related hardware and software. Directory services for that organization remains in place until the Midrange tower and Desktop towers migrate desktops, file servers and other application servers, which will closely

Process	Description
	coincide with the messaging system migrations. Applications directly embedded into the legacy messaging system will have a smaller infrastructure left in place to continue those operations for the agency, like Lotus Notes Servers. The operations staff continues to support any infrastructure left in place. This legacy support is not expected to be a large level of effort because it will include systems that have application developers supporting the application. Legacy systems retired will be considered unrecoverable and Commonwealth approval is required in order to have them removed from production.
Data center move	When the Commonwealth Partner's data center is prepared we will perform a data center move from the RPB data center to our new data center.
Staff messaging data center move team.	The Commonwealth Partners will staff an experienced team of architects and consultants to perform the data center move.
Setup SAN replication with new data center SAN.	The data that has been migrated to the RPB data center SAN, including the server operating systems, is replicated to the duplicate SAN in the new data center.
Setup servers on new data center SAN.	New X-Series servers are installed and configured against the new data center SAN. These servers will be using the same partition configuration as the live servers in the RPB data center. All other infrastructure servers like Domain Controllers, Outlook Web Access servers, and Live Communication Server will be rebuilt and tied to the existing infrastructure over the WAN. The operations team will assist the data center move team with these build outs as necessary to fit within a 4 month transition timeframe.
Test all functions possible.	Test all functions possible, including OWA servers, Live Communication Servers, etc.
Setup new live Exchange 2003 cluster in new data center to continue migrations.	New Exchange hosting services will be created in the new data center so the migration team can continue to migrate data to these servers.
Turn off the Exchange servers in the RPB data center, turn on duplicate Exchange servers in the new data center.	The server operating systems, configurations, and databases will be exactly duplicated in the new data center. When these servers are turned on they will in effect become the exact same servers as those in the RPB data center. After a short overnight outage, because of changing IP addressing and name resolutions, end users will not know any change happened, and migrations will never be interrupted.

Figure 11.3.7 - 5 Depicts the advanced and detailed process the Commonwealth Partners will follow to for 100% success in agency migrations within 2 years.

Service Offerings and Assumptions

The Commonwealth Partners offer a comprehensive service model that fully meets or exceeds the Commonwealth's defined messaging requirements. This model provides high levels of system uptime, excellent system performance, and improved user productivity. The following tables describe the service offerings and demonstrates how the solution components fit together to complete the Commonwealth's messaging and directory services. The first table illustrates those components within the base offering. The second table illustrates those solutions that are not part of the base offering, but can be added at a per user choice by the agencies.

Description	Requirements	Functional Details, Limitations, and Assumptions
Services needed to migrate users from legacy systems to new systems.	Minimum supported workstations need Windows 95 with Active Directory Client Extensions installed and Outlook 2000 or better.	<ul style="list-style-type: none"> • Encrypted Mail messages within legacy systems decrypted before migration. • Classroom training from the Commonwealth Partners on Outlook use is not required.
	Migration team migrates legacy server side mail data to the new mailbox for the users during overnight periods.	<ul style="list-style-type: none"> • Legacy systems cannot be retired until the Commonwealth approves. • No more than 40 MB of data will be migrated. • Distribution Lists, Inbox Data, Calendar Information, Contact Information and Task Information will be migrated.
	Migration team notifies agency of individual users getting migrated at least one week prior to those migrations, unless otherwise approved by the Commonwealth.	<ul style="list-style-type: none"> • Users receive instructions and information regarding their migration via e-mail within their legacy system. • Users with encrypted mail in their mailbox will be able to follow the decryption instructions provided in the above message.
Services that provide user authentication, user attributes, and other metadata about the environment.	The Commonwealth Partners provide a single forest/single domain Active Directory architecture for the Commonwealth's shared use.	<ul style="list-style-type: none"> • A single forest/single domain model is sufficient to provide all the security required by all agencies. • Agencies are willing to use logical security to secure the data they desire. Firewalls, file access control lists, and IPSEC encryption are sufficient for security purposes. • If additional security measures need to be introduced to the solution to solve security issues related to the single forest/single domain model, they can be introduced. • Password complexity, account lockout, and other password related policies could be the same throughout the Commonwealth's agencies. • If password policies cannot be the same across all agencies, a single forest/multiple domain model can be implemented.

Description	Requirements	Functional Details, Limitations, and Assumptions
	All Active Directory controllers will be centralized.	<ul style="list-style-type: none"> • If a suitable secondary site is available to host domain controllers, some will be kept there for resiliency. • No Active Directory resources will be outside of the data center, except for workstations and users. • Where Active Directory resources, other than desktops, need to be located outside of the physical data center, two local domain controllers can be added to the solution.
	The Commonwealth Partners provides role based administration tools to provision and de-provision user accounts inside the Active Directory, and mailboxes within Exchange 2003.	<ul style="list-style-type: none"> • Delegation of the provisioning to the Help Desk is acceptable. • Auditing and monitoring performed by the operations team to ensure accounts are setup correctly.
	Distribution List Management	<ul style="list-style-type: none"> • Membership management of a static distribution list will be delegated to the end user owner of that list and the Help Desk.
	Security Group Management	<ul style="list-style-type: none"> • All Microsoft based servers joins the Active Directory in the new environment. • Security groups for Microsoft based systems will be in the Active Directory. • The necessary delegations will be made within the Active Directory to allow the appropriate tower to control the security group memberships. • No local user accounts will be used on servers.
	Group Policy Object Management	<ul style="list-style-type: none"> • Group Policy Object management will be delegated to the appropriate tower for control over their own GPOs. • Example: the Desktop tower manages and owns the workstation GPOs for all agencies and any other GPO that effects the user's desktop environment.

Description	Requirements	Functional Details, Limitations, and Assumptions
Services surrounding email, real-time collaboration, mailbox management, antivirus for email, SPAM, and others.	Mailbox size restriction policies	<ul style="list-style-type: none"> • The agency selects the mailbox size limit for all employees in their organization; base assumption is 40MB per user. Individual increases are possible, allowing agencies complete flexibility on disk space allocations. • Reporting and chargeback capability based on these limits will be provided. • SAN disk space allocated with 20% excess space, based on the mailbox size limit chose.
	Mailbox management	<ul style="list-style-type: none"> • 200 mailboxes will be in each Exchange database. There are 20 Exchange databases per server, allowing for 4,000 mailboxes per server. • Agencies that number less than 200 share a database with other agencies. There is no security risk associated with this sharing. • Additional servers and disk space can be added to the baseline solution to allow for dedicated agency databases if deemed necessary.
	SMTP Proxy Address management	<ul style="list-style-type: none"> • The operations team provides backward support for the users legacy SMTP email address. • The default SMTP address space based upon VITA's naming convention will be put on all user objects. (It is not required that all agencies or people use this as their primary SMTP address.)
	Outlook Clients	<ul style="list-style-type: none"> • Outlook 2000 is supported, but Outlook 2003 is recommended wherever possible. • Outlook 2003 will be in a "local cache" mode. • The operations team supports Outlook 2003 as it relates to interoperation with Exchange 2003.

Description	Requirements	Functional Details, Limitations, and Assumptions
	Antivirus and Antispam	<ul style="list-style-type: none"> • Ironport C60 devices provide Internet filters for SPAM and Viruses using Brightmail and SOPHOs software. • Symantec for Exchange 2003 will be used on the internal servers to provide antivirus protection internally. • There will be no need for SPAM filtering on the internal system.
	POP3/s and IMAP4/s	<ul style="list-style-type: none"> • POP and IMAP services available if any agency requires, both internally and externally. • SSL used to secure these protocols. • This service can be provided to specific users, as agencies require.
	Public Folders	<ul style="list-style-type: none"> • A 4-node Exchange 2003 cluster will be dedicated for Public Folder use. • Each agency receives a secured folder inside the public folder structure. • Administration of public folders will be delegated to an assigned agency employee. • The assigned agency employee receives basic instruction on how to administer the public folders remotely. • The operations team supports these delegations and supports users as necessary. • The operations team replicates the public folders database to all three active nodes within the four-node cluster. • Public Folder usage is limited. • Any agency requiring significant public folder usage is recommended to add Sharepoint Portal Services to the baseline solution.

Description	Requirements	Functional Details, Limitations, and Assumptions
	Backup and Restore	<ul style="list-style-type: none"> Full backups of the existing databases in Exchange occur using “snapshot” methods on the SAN, on a daily basis. The “snapshots” backed up by Tivoli Storage Manager to tape as conducted by the Midrange tower. Tapes rotated offsite, as conducted by the Midrange tower. There is a maximum 24 hour data loss tolerance

Figure 11.3.7-6 - Service offerings as part of the base offering and demonstrates how the solution components fit together to complete the Commonwealth’s messaging and directory services.

Description	Requirements	Functional Details, Limitations, and Assumptions
	Outlook Web Access (OWA)	<ul style="list-style-type: none"> OWA provided for connections both inside and outside of the Commonwealth’s data center. SSL secures the authentication and data for connections. Forms based authentication enabled to increase security. Secure web proxies used to access OWA from the Internet. This service can be provided to specific users, as agencies require.
	Exchange Based Custom Applications	<ul style="list-style-type: none"> Legacy Exchange based applications ported to this new system if determined necessary by the Commonwealth. New Exchange based applications will not be supported. Sharepoint Portal Services can be added to the solution to provide for these types of applications reducing dependencies and decreasing long-term support costs.
	Application integration and support	<ul style="list-style-type: none"> Directly integrating applications using Exchange Application Programming Interfaces will not be supported.

Description	Requirements	Functional Details, Limitations, and Assumptions
		<ul style="list-style-type: none"> Integration of applications using LDAP or SMTP is fully supported and encouraged.
	Wireless Email	<ul style="list-style-type: none"> Blackberry Devices are the supported client type for wireless email access.
	Secure Messaging	<ul style="list-style-type: none"> Per user SSL certificates will be added to the solution for those users or agencies that require the ability to encrypt email messages in the Outlook clients, or OWA. This capability is not required for every user.
	Real-Time Collaboration Services	<ul style="list-style-type: none"> Live Communication Server 2005 is the solution to provide these services. Not all Commonwealth users or agencies will use this service. It can be provisioned on a per user basis. Ad hoc online meetings using this system fill the “online meeting” requirement If formal online meetings are required, Microsoft Live Meeting can be added to the solution. Users that require the service must have Windows XP desktops with Office 2003, and Microsoft Communicator or Windows Messenger 5.1 or better.
Archives email, scans email for inappropriate use, and allows for legal discovery searches of archived email.	Assentor Compliance Services	<ul style="list-style-type: none"> Available on a per user basis. Scans emails with Commonwealth predefined filters for inappropriate use. This is the “Compliance Service” definition within the SOW requirements. The Commonwealth Partners will not recommend filters, or view emails discovered to be non-compliant. Mechanisms will be put in place so VITA or agency management will be directly alerted to inappropriate use.
	Assentor Mailbox Manager archive	<ul style="list-style-type: none"> Available on a per user basis

Description	Requirements	Functional Details, Limitations, and Assumptions
	services	<ul style="list-style-type: none"> Archives user mailboxes to a central database and allows those users to access and search the archived email. The Commonwealth Partners provides support for these archives as if they were mailbox extensions. This answers the SOW requirement of email archiving.
	Assentor Discovery Services	<ul style="list-style-type: none"> Available on a per user basis Archives user email to a central database and provides a detailed search capability for legal investigations, or other investigation. The Commonwealth Partners provide support to the agency or legal group requiring the ability to search emails. The Commonwealth Partners will not perform actual searches, or provide personnel to filter or read actual data. Because of potential sensitivities to this data, searches will not be supported by the Commonwealth Partners unless a formal approval comes from the VITA CIO or VITA legal group and it is confirmed by the Commonwealth Partners legal groups. This is part of the SOW requirement for compliance services and archiving.
Monitors the environment for bottlenecks and alerts the appropriate operations team members for attention. Reports on usage statistics for charge backs, total cost of ownership reports, and other reporting	Quest Software Active Directory and Exchange Monitoring tools	<ul style="list-style-type: none"> Tools provide data feed to the Commonwealth Partners charge back solution. Tools provide appropriate alerts to NOC, Help Desk, and operations teams on potential bottlenecks or threshold breaks. The Commonwealth and the Commonwealth Partners agree upon details of SLA thresholds.

Description	Requirements	Functional Details, Limitations, and Assumptions
functions.		
Solutions details not provided in the Commonwealth Partners messaging solution; however services provided for can be enhanced in the future using these Value Add components.	Messaging Services	<ul style="list-style-type: none"> • Users can be provided with RPC over HTTPs access to their email over the Internet. Users with Outlook 2003 on their home machines can use the full client instead of OWA, and get the full functionality of Outlook as if they were at their desk. • Smartphones using Windows Mobile 2002 or PocketPC can access Outlook Mobile Access if additional wireless services beyond Blackberry are required.
	Real-time Collaboration Services	<ul style="list-style-type: none"> • Microsoft Live Meeting can be integrated into the Live Communication Server solution to provide a more formal online meeting workspace. • Video solutions can be introduced to integrate with Live Communication Server. • Live Communication Server can integrate with Voice Over IP to support any unified messaging solution. • External connectors can be added to Live Communication Server to provide bridged connection to MSN, Yahoo, or AOL instant messaging solutions. • Users can access Live Communication Server from their home using Microsoft Communicator or Windows Messenger 5.1 or better. This allows them to chat and collaborate with co-workers from home. • Sharepoint Portal services can be added to the solution to provide an application platform. The use of XML standards makes the solution very open, and it will integrate well with Active Directory, Exchange 2003, and Live Communication Server 2005.

Figure 11.3.7-7 - Service offerings that are not part of the base offering, but can be added at a per user choice by the agencies. This table also demonstrates how the solution components fit together to complete the Commonwealth's messaging and directory services.

Technical Architecture - Overview

The architecture of the Commonwealth Partners solution is comprehensive and extremely scalable. Figure 11.3.7 - 8 depicts the overarching solution with all the configurations shown. The number of servers and devices within the figure are not exact to the complete solution; however, the figure shows how the solution could scale, both up and out. The grey servers show the initial configuration, and the blue servers indicate the servers that will be added as users are brought into the system.

The physical server architecture will be comprised of IBM X-Series quad processor servers with 4 gigabytes of RAM for each server. This allows for the maximum number of user support for each service within the solution. Each server service will also be load balanced or clustered for redundancy, based on the application functionality. The scaling and redundancy of the solution is shown in the table below.

Solution	Users Per Server	Redundancy
Exchange Server 2003 Back-End Servers	12,000	4-Node Cluster (Active/Active/Active/Passive)
Exchange Server 2003 Front-End Servers	24,000	2 - Load Balanced hosts Scaled number based on use
* Live Communication Server 2005	100,000	2 – Load Balanced host servers 2 – Load Balanced Access Proxies if service is chosen 2-Node Cluster for database
Active Directory Domain Controllers	4,000	Up to 20 servers using native replication for redundancy
RIM Blackberry Enterprise Servers	1,000	2 – Servers, one active, one passive
Ironport C60 SMTP Gateways	70,000	3 – Devices Load Balanced
Web Proxy Services	24,000	2 – Load Balanced Scaled number based on use
* Illumin Assentor Enterprise Mailbox Archiving per user	4,300	2 – Load Balanced Scaled number based on use
* Illumin Assentor Enterprise processing servers	70,000	5 – Load Balanced mail processing servers
* Illumin Assentor Enterprise back end servers	70,000	5 Compliance Server 1 Archive Server 15 Mailbox Archiving Servers 2 Database Servers (Clustered)

*Indicates solutions that are not part of the base offering, but can be added at a per user choice by the agencies.

Figure 11.3.7 - 8 Shows scaling and redundancy of the solution

Technical Overview – Active Directory

Microsoft Active Directory Domain Architecture

Microsoft Active Directory 2003 is an extremely scalable directory solution that lends itself to large scale consolidations such as the Commonwealth agencies. Active Directory itself can support well over 1 million objects inside of it and many different organizations, each with its own unique set of operational requirements.

The Commonwealth has approximately 70,000 users meaning the number of objects within the Active Directory will be far fewer than 1 million objects. The reduced numbers of users allows the Commonwealth Partners to implement a single forest and single domain baseline model. Organizational Units (OUs) will be created to keep a logical administrative separation between agencies, users, workstations, and enterprise services like Exchange Server 2003. This allows for delegated Group Policy Objects (GPOs) to manage the different security and other requirements on the different objects within the directory so the Commonwealth agencies will have the flexibility to define their own business requirements on systems without affecting other agencies. Figure 11.3.7 - 9 shows the flexibility of Active Directory and how the Commonwealth Partners will use GPOs to manage the different agency business requirements.

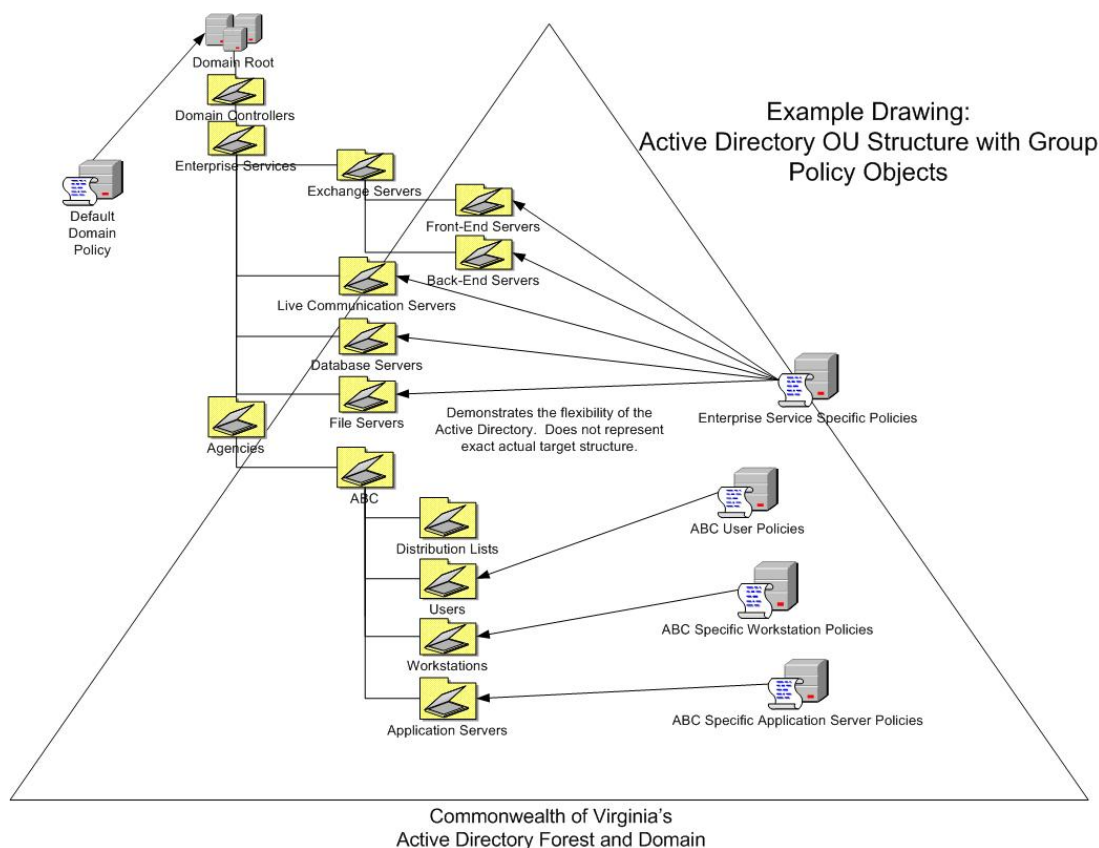


Figure 11.3.7 - 9 Shows the flexibility of Active Directory and how the Commonwealth Partners will use GPOs to manage the different agency business requirement.

As mentioned, Active Directory uses Group Policy Objects (GPOs) to manage collections of objects within the directory. The default domain policy is one of those policies; it enforces password policies with definitions like the account lockout policy, account lockout duration, password complexity requirements, and number of historical passwords the system should remember. This policy is the first layer of

protection for any organization and should be as strict as can be reasonably supported. It is expected that VITA and the agencies will come to an agreed upon common password policy for the entire Enterprise, as it allows for the simplest support and administrative models, thus reducing Total Cost of Ownership. If an agreement is not met by VITA and the agencies the Commonwealth Partners can add to its baseline model the necessary architecture, design, software and hardware to support any new requirement. Figure 11.3.7 - 10 depicts how the Commonwealth Partners will scale out its baseline Active Directory model in order to provide the highest levels of security and flexibility to any new VITA domain requirement and, still provide the required centralized messaging solution.

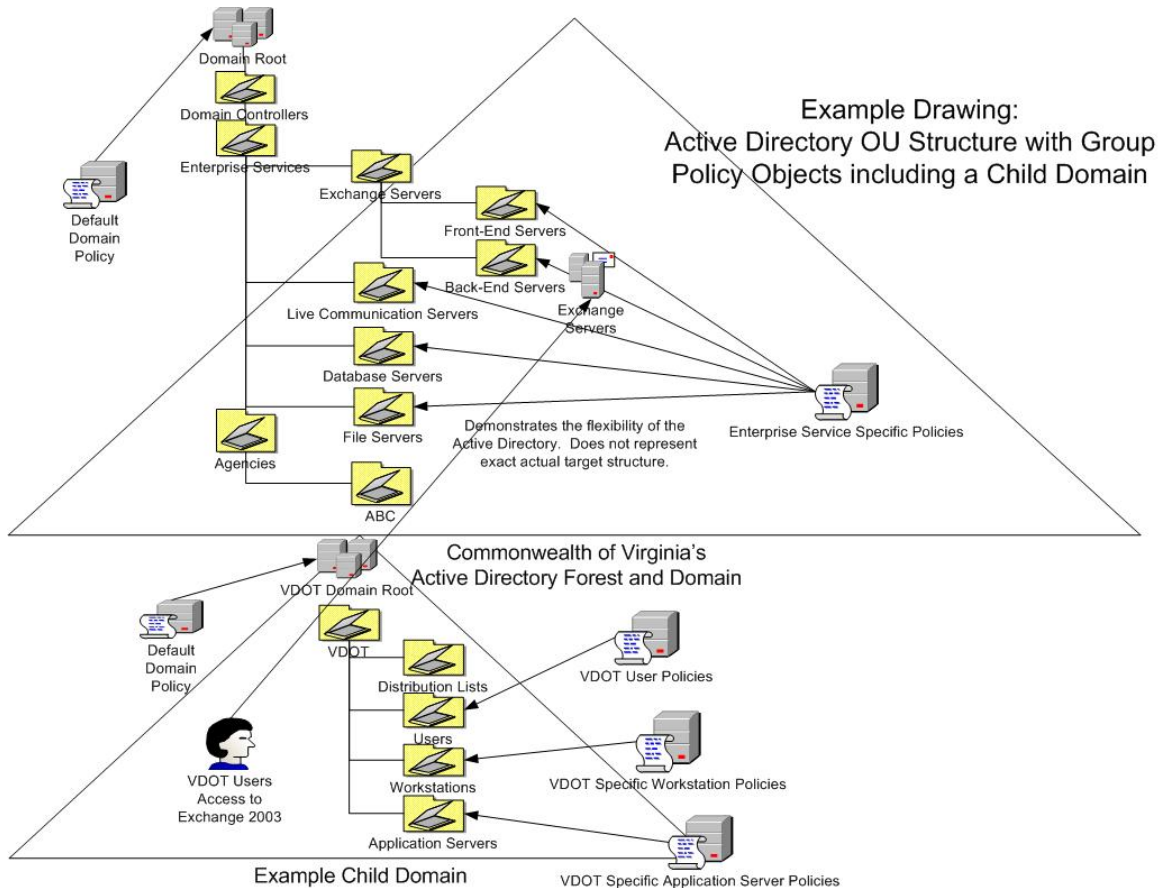


Figure 11.3.7 - 10 Shows the Commonwealth Partners will provide the highest levels of security and flexibility to any VITA domain requirement

Microsoft Active Directory Global Catalog and other Exchange related functions

Active Directory has a large percentage of shared functionality with Exchange Server 2003, for instance the directory contains all the information necessary for the Exchange Global Address List (GAL). This function of the Active Directory is called the Global Catalog service and will be enabled on almost all the domain controllers within the Commonwealth data center. This ensures users needing information from the GAL have faster access, as there will be up to 18 Active Directory controller servers within the environment with each server supporting over 4,000 active user connections. These servers are also the authentication servers for all logons to the domain from all agencies, as file servers, workstations, and other Microsoft based services are migrated to the centralized solution by the other Commonwealth Partner towers, these Active Directory Controllers will be able to support the additional loads with no

performance issues. The Messaging Services team will monitor them closely to ensure the Active Directory is functioning, and stable at all times.

The Active Directory also stores all the proxy address information for each user that has an Exchange mailbox within the organization, though Exchange 2003 manages those SMTP proxy addresses. The addresses of the agencies within this solution do not need to be altered from their current namespaces. In other words, a new root VITA SMTP address will be added to each user, however their old SMTP email address will still be supported. This means users will not have to change business card email addresses unless they so desire, nor will they have to worry about calling all their contacts to tell them of an address change.

The Active Directory is also responsible for distribution list storage and membership. The messaging tower configures new distribution lists based on agency and VITA requirements, as well as maintains those distribution lists that agencies use today. These lists, where appropriate, will be secured so only the appropriate people can send email to them, or change their membership by using Outlook on their desktops. Membership of these lists can be hidden from all users to maintain security as well. Dynamic distribution lists are available in the 2003 version release of Active Directory and Exchange. These lists do not have explicitly defined members, but instead they are dynamically built from attributes within the Active Directories' user objects at the time a message is sent. This allows for the lists that encompass all users within an agency to be 100% accurate at all times because each user will have the agency name in their user object attributes. These "all agency" user lists can then be nested inside an entire "All Commonwealth Users" distribution list, which then has a high confidence of correct and full membership at any given time.

Microsoft Active Directory backup and restore

The Active Directory controllers will be backed up on a daily basis to ensure that there is a full restoration copy available at any time of disaster. Quest Software's Recovery Manager for Active Directory is being implemented by the Commonwealth Partners to ensure the ability to quickly recover data to Active Directory, without service disruption. The tool uses the backups made by the Commonwealth Partners to retrieve and re-write all the removed objects back to their original conditions, taking into account how they need to be replicated back into the other Active Directory domain controller servers.

Microsoft Active Directory monitoring

The Active Directory will be monitored closely by the messaging and directory team, which will employ an automated set of tools from Quest Software. The primary Active Directory monitoring tool will be Spotlight on Active Directory. This tool will check the replication of the directory on all domain controllers to ensure they are up to date and available to be updated on the next replication. This tool will also monitor thresholds and send alerts related to domain controller bottlenecks and replication problems. These alerts can interface with any of the Commonwealth Partners systems, from the Help Desk to the NOC, in order to ensure alerts are received, tracked and managed correctly. This will ensure the service levels regarding Active Directory are measured and reported.

Microsoft Active Directory migration tools

Quest Software's migration tools will be used to migrate the existing Microsoft, Novell, and Notes systems to the new centralized Microsoft Active Directory and Exchange environments. The Quest tools automate the migration of one directory to another directory while allowing for seamless fall back in the case of issues being encountered. The best practice migration is a "copy" of user objects from one directory to the other. The email attributes that point email to the correct location are not changed within the objects until the user is migrated. The tools and scripts used to migrate the user can quickly undo these changes within the user attributes to allow for minimum risk and loss of service or data in the migration process. These tools also include the ability to change Outlook profiles remotely.

Microsoft Active Directory security

Microsoft Active Directory is secure by design and default. The directory requires Kerberos 5 authentication and NTLMv2 for back level clients, to be used whenever access to any resource is requested. Lightweight Directory Access Protocol (LDAP) signing is used when the lower level of the directory is accessed using that protocol, so even custom applications using LDAP are secured with zero effort. These implementations of encryption ensure that authentication data is secured within the Active Directory environment. In addition, wherever the business requirements dictate, Internet Protocol Security (IPSEC) can be added to the solution to ensure server to server or client to server data is encrypted, for example OWA server communications with back end Exchange mailbox servers. This can be done using the GPOs mentioned earlier and the Commonwealth Partners can implement it on a server-by-server basis where agencies require it. Windows XP will be a requirement on workstations that need to access a server that has IPSEC enabled.

Microsoft Active Directory physical domain controllers

Active Directory controllers will be all physically located within the Commonwealth's RPB current data center, until such time a new data center is created by the Commonwealth Partners. All domain controllers will be replicated to new servers within the new data center to ensure zero service outages for this data center move. If a suitable offsite location can be agreed upon between the Commonwealth and its partners, 3 or 4 domain controllers will be operated and remotely administered in that location for resiliency.

Technical Overview – Exchange 2003

Microsoft Exchange Server 2003 Storage configuration

Microsoft Exchange Server 2003 will be used as the core messaging system for the Commonwealth. This robust system allows for more than 4,000 users per server. The Commonwealth's current 270 messaging related servers will be reduced to less than 100 servers, while new services like real-time collaboration and archiving are added. This is a 60% reduction in messaging servers for the entire Commonwealth of Virginia.

Each Microsoft Exchange Server will be in a 4-node cluster with three active servers and one passive server standing by in case one of the active servers fail. Windows Server 2003 supports up to 8-nodes within a single cluster, therefore the solution can scale quickly to any growth rate. Up to six of these 4-node Exchange 2003 clusters will be required to support the expected 69,000+ users in the Commonwealth agencies. The Commonwealth Partners will configure one additional Public Folder cluster starting with 2-nodes and scaling up to 4-nodes when required.

Exchange Server 2003 supports up to four storage groups with five database stores per storage group. The Commonwealth Partners will work directly with VITA requirements and guidance on how these storage groups and databases should be used across all agencies. The baseline model assumes that agencies will share databases, storage groups, and servers.

The Commonwealth Partners also will be using technology newly available and proven within Windows Server 2003. This technology is the use of "mount points" instead of logical drive letters as in the past. Previous versions of Windows did not have this ability; therefore each Exchange storage group had to receive its own logical drive letter. These drive letters would then contain a large partition to hold all the five supported databases for that storage group. The partition holding these databases could possibly fill with data, or require increased partition size due to quota increases, causing administrators to take all five databases within the storage group out of service while additional disk space is added. By using "mount points" this issue becomes a thing of the past. The storage group will be put onto a logical drive as before, but the only data on this logical drive will be five "mount points", one for each individual database within

the storage group. If one of the “mount points” were to need additional space added, only that individual database would have to be taken out of service to add the space to the system. This drastically decreases the number of users affected when performing disk level maintenance on the Exchange servers and allows for a more dynamic scaling of the disk space. Figure 11.3.7 - 11 shows the creative use of new technology for maximizing the uptime of the Commonwealth’s messaging infrastructure.

Figure 11.3.7 - 11 Shows configuration of the new technologies to maximize uptime

Internet and Wireless Client Access

Agencies will have a large list of flexible connection methods from the Internet to their internal email boxes. Baseline service offerings of connections include:

- Outlook Web Access over SSL (HTTP/s)
- POP3/s or IMAP4/s
- Blackberry wireless services

Additional connection options can be added to the baseline solution by VITA and the Commonwealth if the type of connection is desired:

- RPC over HTTP/s for use with Outlook 2003 over the Internet.
- Outlook Mobile Access over SLL for Smartphone devices that support it.
- Live Communication Services over the Internet over the Internet through Access Proxy Servers

As noted all of these connections will be secured using Secure Socket Layer (SSL) certificates from Verisign.

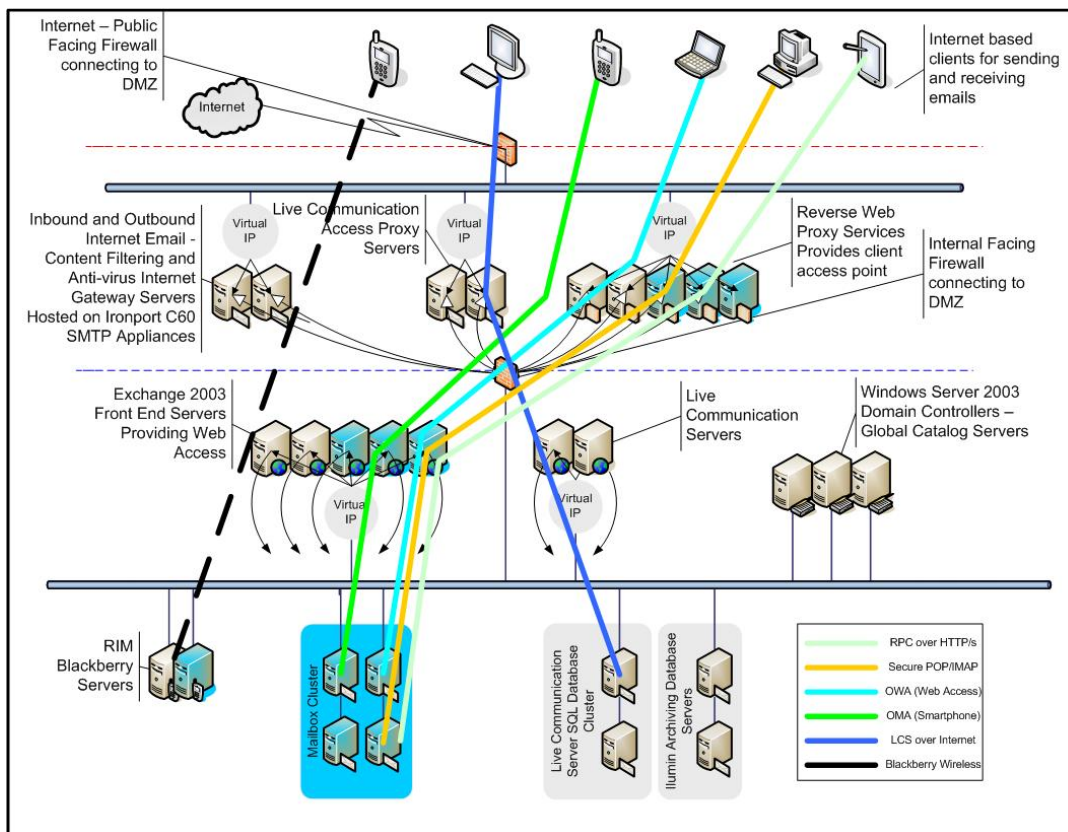


Figure 11.3.7 - 12 Identifies the flexibility of connection types that can be offered securely by Commonwealth Partners messaging solution, giving its employees the ultimate flexibility in communicating from anywhere at anytime.

Exchange 2003 Monitoring and Management

Quest Software's management tools for Exchange and Active Directory will offer extended capabilities to provide the Commonwealth with the required reporting and SLA monitoring.

- Quest MessageStats provides quantitative real world data, which shows the use of the Exchange 2003 systems. The software will provide the following types of reports, many of which are included in the sample reports requested by the Commonwealth's SOW.
 - Mailbox sizes by agency or department.
 - Messages sent and received by specific agencies, departments or personnel to include message size, message volume and other metrics.
 - Chargeback reports based on mailbox size.
 - Distribution List Membership reporting.
 - Mailbox Quota Reports.
 - Top Internet domains that email has been sent to and received from.
 - Trending graphs on the amount of messages sent and received over long periods of time, months or even years.
 - Average server delivery times.
 - Message sizes sent to distribution lists.

All of these reports allow for detailed analysis of the Commonwealth's email system to understand any bottlenecks that have developed, misuse of the system, SLA for message delivery, and more. A proactive example of this tool is to have the help desk run the Mailbox Quota report on a weekly or monthly basis. This process identifies users that are close to running out of mailbox space. These users could be contacted before they are presented with the automated system message stating they are running out of space. This means the help desk can call a user before the user calls the help desk. The following figure shows the Mailbox Quota report and how the Commonwealth can use this report to proactively assist the Commonwealth's end users.

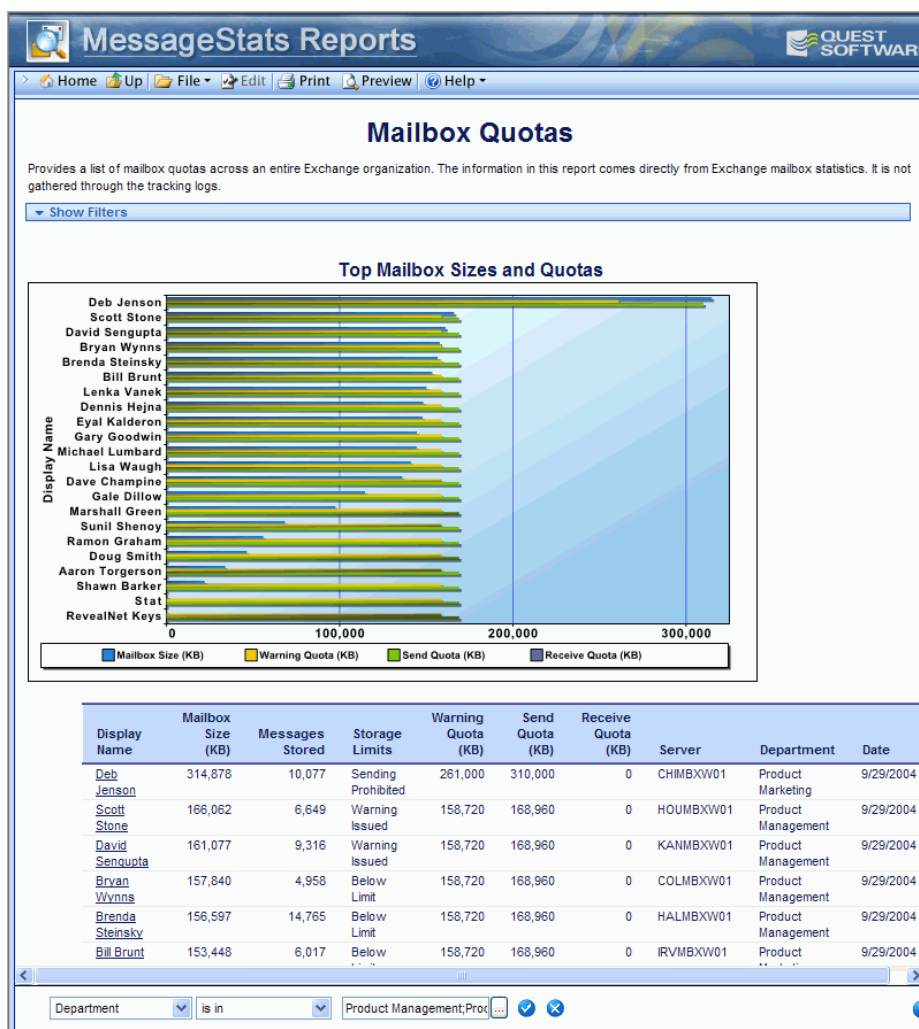


Figure 11.3.7 -13 Quest Mailbox Quota Report used to proactively manage mailbox limits

Quest Spotlight on Exchange is a robust monitoring tool for Exchange and it allows for scheduled test messages to be sent to different servers to ensure adequate delivery times and detect possible problems. This tool alerts the Commonwealth Partners to messaging issues before they become a systematic problem. The tool can also interface with third party applications so Help Desk tickets can be generated automatically or alerts sent to the NOC depending on the rule sets defined by the Commonwealth and its Partners.

Internet SMTP, SPAM, and Antivirus Services

Ironport C60 devices will be configured to send and receive email to and from the Internet using the SMTP protocol. Brightmail SPAM filtering eliminates up to 60 percent or more of SPAM email traffic on the Internet from entering the Commonwealth's messaging system thus reducing costs of storage and saving the employee's time in filtering through email messages. Anti-Virus protection comes from one of the leading anti-virus providers on the market, Sophos. This product catches all incoming messages with viruses and removes the offending code safely. Ironport also includes the virus outbreak filter that finds new viruses not already identified by the industry. Symantec provides antivirus protection services on the internal Exchange 2003 servers to create a defense in depth antivirus strategy.

Microsoft Live Communication Server 2005 configuration

Microsoft Live Communication Server 2005 is an extremely scalable and capable real-time collaboration tool meant for the enterprise. The configuration consists of two client connection servers in a load-balanced configuration and two Microsoft SQL 2000 Enterprise servers in a two-node cluster configuration. This configuration provides an archiving database and configuration database to store user's buddy list and other metadata information, which will be backed up on a daily basis. Live Communication Server 2005 integrates directly with Active Directory to allow for easy user-by-user provisioning of the service. As depicted in Figure 11.3.7 – 10above, two additional servers can be added to the baseline configuration to support access to the solution from the Internet.

Microsoft Live Communication Server 2005 Presence Detection

Integrating presence with the Microsoft Office System is unique to Live Communications Server. Rather than forcing people to break concentration in order to get the information they need to complete their work, Live Communications Server provides in-context communication to keep workers on task and increase their productivity. Workers may instantly find and communicate with people from within familiar programs such as Microsoft Outlook, Microsoft Excel and Microsoft Word. This integration occurs wherever the user sees a “paw”, the icon representing a person's presence status. When co-workers have accurate information about team members' availability, they do not waste time trying to contact them through inappropriate means. This translates into increased productivity and frequently reduces costs as well.

Several people can work or provide comments on the same document; eliminating multiple outdated versions and cluttered e-mail strings.

To support these scenarios, SharePoint offers presence awareness throughout its interface. Presence icons show up in lists and XML-based Web parts. Meeting Workspaces, if SharePoint is added to the Commonwealth Partners solution, provide dynamic presence icons next to each team member's name. Member Lists, with presence icons for each person who is a member of that SharePoint site, are also conveniently visible to the users.

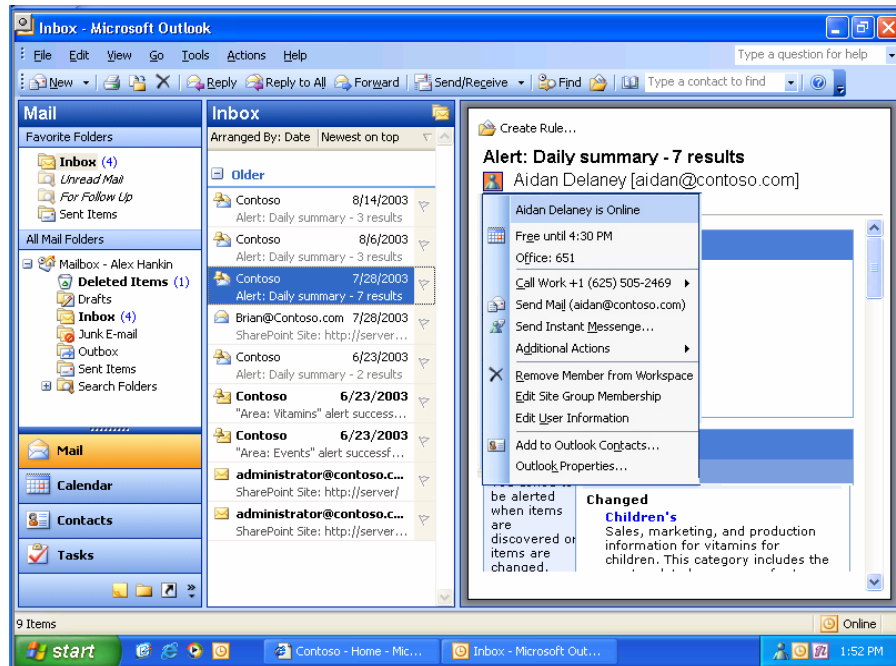


Figure 11.3.7 - 14 Demonstrates “presence detection” feature for identifying users online for collaboration

Workers can instantly see who is online and available to discuss documents or upcoming meetings, regardless of time zone or location. With Microsoft® Exchange integration, the user can even check a person’s schedule and get up-to-date availability information directly from their calendar. This makes it easy to determine when someone will be free to communicate.

Presence is integrated into other Microsoft Office System programs through Document Workspaces and Smart Tags. Smart Tags are XML-based tools that recognize certain names, phrases or numbers in Microsoft Word and Excel. The item appears with a subtle dotted red underline, letting the user know there is a range of actions that can be taken instantly with a click of the mouse. Examples include sending e-mail, checking someone’s schedule, initiating an instant message or finding out someone’s job title. Adding presence information to these programs with Live Communications Server allows the user to communicate with relevant people directly within a familiar interface.

The Commonwealth can increase user productivity with integrated presence and real-time communication to locate people and share information quickly.

- Instantly find and collaborate with local and remote users to share critical and time-sensitive information.
- Presence awareness within your desktop and line-of-business applications eliminates delays in locating and communicating with key work partners
- Enable remote users to access security-enhanced presence and instant messaging (IM) solutions without requiring Virtual Private Networking (VPN). Provide mobile workers with access at home or on the road.
- If the LCS External Connector service is added to the Commonwealth’s solution the users can collaborate with other organizations as easily as co-workers while protecting sensitive business information.
- Instant Messaging functionality
- Audio and Video support
- Handwriting messages (Ink Support)
- Application and Whiteboard Sharing
- Desktop Sharing for Remote Assistance
- Point to Point File Transfer

*** Microsoft Products with Presence Powered by Live Communications Server**

***Indicates solutions that are not part of the base offering, but can be added at a per user choice by the agencies.**

Feature	Application
Instant Messaging	Microsoft® Windows Messenger
Collaboration	Microsoft® Office SharePoint Portal Server Microsoft® Windows SharePoint Services Microsoft® Office Live Meeting

Feature	Application
Communication	Microsoft® Outlook Microsoft Exchange Server 2003
Productivity	Microsoft® Excel Microsoft® Word Microsoft® PowerPoint Microsoft® Office Visio Microsoft® Publisher


Figure 11.3.7 - 15 Shows Microsoft products that work with the Live Communications solution























Live Communication Server 2005 has an impressive feature list that shows what Commonwealth can take advantage of today and in the future.

*** Live Communication Server 2005 w/SP1 Enterprise Edition Feature List**

***Indicates solutions that are not part of the base offering, but can be added at a per user choice by the agencies.**

KEY:

-  = Feature Included
-  = Improved in LCS 2005
-  = New in LCS 2005

Microsoft® Office Live Meeting integration		Active user capacity Over 100,000 per server pool	
Share security-enhanced IM and presence between 2 or more organizations (federation)		Scalability planning tools	
Connectivity to MSN, AOL and Yahoo public IM service providers ¹		Failover support for planned growth or unplanned downtime	
Link corporate telephone system and computers (PBX/PSTN integration)		Clustering capability	
Presence status control (online, away, busy)		Archiving and logging	
Do not disturb setting, disabling notifications		Advanced logging	
Server-side or “roaming” contact list		Audio/video and IM text encryption	
Integration with Microsoft Office programs		Kerberos, NT LAN Manager (NTLM) authentication	
Offline status		Protection against unsolicited instant messages (SPIM control filters)	
150+ contacts supported		Manage Live Communications Server 2003 and 2005 servers	
Contact search outside contact list		Support for Microsoft Operations Manager 2000 and 2005 versions and	















		Microsoft Management Console (MMC)	
Microsoft Exchange free/busy information		Active Directory service integration	
Instant messaging (IM)		Group Policy Object management	
Audio and video		Enable users by per-user, bulk-user and per-feature basis	
Handwriting messages (ink support)		Data recovery	
Application- and whiteboard-sharing		XML-based management tools	
Desktop sharing (remote assistance)		Enhanced federation support	
Point-to-point file transfer		Server application programming interface (API)	

Figure 11.3.7 - 16 Shows the Features available with Live Communication Server

*** Illumin Assentor Enterprise Compliance, Archiving, and Discovery Services**

Any enterprise solution is faced with the surge of volumes and dependencies on email, enterprise messaging systems have become business-critical knowledge repositories for many organizations. As information stores continue to rapidly grow, the Commonwealth Partners need to manage the size and performance of the Exchange 2003 servers without taking critical content away from the user base. However, to manage the information stores, organizations typically either rely on email quotas or move files to personal archives (PSTs). In either case, important data is either deleted or at a high risk of being lost.

Larger information stores are costly if not managed properly. Typical organizations must incur the high operational expenses of backup media and management as well as managing personal archives. Below is a list of operational efficiencies delivered by Illumin Assentor Enterprise giving the Commonwealth a rapid return on investment as well as lowering the total cost of ownership of the messaging system.

- Eliminates the growth of expensive storage and actively manages system data
 - Higher reliability
 - Higher performance
 - Faster backup
 - Faster restore
 - Faster upgrades
- Increases the accessibility through a centralized search
- Manages retention, storage migration and eventual deletion
- Different service levels can be implemented for archive data
- Vital data is not lost
- End users can quickly access all archived and non-archived email

The overall physical layout of this service greatly depends upon demand and use of the service. Initially it is expected to require approximately 5 servers for minimum requirements.

*** Illumin Assentor Compliance Services**

The compliance scanning servers are a simple load balanced array of servers that take data from the Exchange 2003 servers and review the content as designed. Initially two servers will be used for the solution, however servers can be added to the solution as demand and usage requires. In full service for the Commonwealth, only five or six servers would be required.

These services provide the Commonwealth with data on inappropriate use of email. The service is delivered per user and scans emails based upon a set of rules the Commonwealth will define. There is industry best practice filters provided from Illumin to give the Commonwealth a head start on what to look for in compliance service filtering. While the Commonwealth Partners implement and manage the technology, the Commonwealth's employees and managers review the data and determine action.

*** Illumin Assentor Mailbox Manager Archiving Services**

The solution begins with two archiving servers in a load-balanced configuration pulling email from the specified users mailboxes on the Exchange server and storing those email messages and attachments in a single instance storage database. A pointer to the message will be left within the users Exchange mailbox, so they do not experience any loss of data. This solution provides the Commonwealth users selected for the service with what can become "unlimited" mailboxes, depending on how long the Commonwealth chooses to retain the archived information.

*** Illumin Assentor Discovery Services**

The Commonwealth Partners can make available, on a per user basis, discovery services allowing legal groups or internal agency investigators to search archived email and return those results for delivery to the concerned parties. This technology can be made available whether or not the compliance or archiving solution is selected. The Commonwealth Partners will not conduct searches on the data for the Commonwealth; instead Commonwealth employees should be used. Searches will need to be authorized through the legal agencies within the Commonwealth and the Commonwealth Partners organizations.

Benefits of the solution include more reliable messaging services, increased security, productivity, flexibility, and an ability to move into the future with lower costs per user based on the level of services provided.

The users that require cross agency communication will find the common directory accurate and dependable. The flexibility in access to the system through the leveraging of web-based solutions allows for any end user to communicate with the people they need to, wherever they are located. The highly available configurations at all levels of the solution ensure users can communicate with each other anytime, day or night.

***Indicates solutions that are not part of the base offering, but can be added at a per user choice by the agencies.**

Conclusion

The Commonwealth Partners bring a centralized and flexible messaging service to the Commonwealth end user community. These back end messaging services allow the end users of the Commonwealth to become more effective in their communication with each other as they will be using Microsoft's productivity toolsets at the local desktop to integrate into this solution. They will locate coworkers in the system that they need to communicate with much faster, they will be able to share information and collaborate with those coworkers in a much more efficient manner, and they will have more time to provide services to Commonwealth citizens.